Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

CHARACTERISTIC SUBGROUPS OF AN ABELIAN PRIME POWER GROUP.

By G. A. Miller.

§ 1. *Introduction.*

A subgroup which corresponds to itself in every possible automorphism of a given group is called a characteristic subgroup or an I-invariant subgroup. Some fundamental properties of the characteristic subgroups of any abelian group were studied by the writer of the present article in a paper published in volume 27 of the American Journal of Mathematics, 1905, pages 15–24. In particular, it was noted in this paper that besides the identity there is a certain characteristic subgroup, called the fundamental characteristic subgroup, which appears in every possible characteristic subgroup of an abelian group G whose order is of the form p^m, p being some prime number.

The present paper is devoted to a determination of various new properties of the characteristic subgroups of G. For the sake of clearness it seems desirable to explain here a few terms which are frequently employed. Two groups H_1 and H_2 are said to be complementary groups as regards a group G provided at least one H_1 of these two groups is an invariant subgroup of G while the other H_2 is simply isomorphic with the quotient group of G with respect to H_1. When G is abelian it is known that H_2 is simply isomorphic with at least one subgroup of G and hence it is convenient to speak of *complementary subgroups of G. Two invariant subgroups H_1 and H_2 are said to be complementary subgroups of a group G provided each of these subgroups is simply isomorphic with the quotient group of G with respect to the other.*

It should first be noted that if one of two subgroups of G is simply isomorphic with the quotient group of G with respect to the other the two subgroups are not necessarily complementary. For instance, every subgroup of order p is simply isomorphic with each of the quotient groups arising from the subgroups of index p, but when G involves λ distinct invariants the quotient groups arising from its subgroups of order p are of λ distinct types. Each of these types corresponds to one set of I-conjugate subgroups of order p. That is, there are just λ sets of I-conjugate complementary subgroups of order and of index p. It will be seen in the following section that these correspond to the λ characteristic subgroups generated by operators of order p, and the λ characteristic subgroups involving operators of order p^{α_1-1}, p^{α_1} being the order of the largest operators contained in G.

The complementary subgroup of the fundamental characteristic subgroup is composed of all the operators of G whose orders divide p^{α_1-1} and it is characterized by the fact that it is the only characteristic subgroup of G which includes every other characteristic subgroup of G. It is the cross-cut of all the subgroups of index p under G which are complementary to the subgroups of order p contained in the fundamental characteristic subgroup of G. It should be noted that the numbers of these complementary subgroups of order and of index p are equal to each other.

The simplest characteristic subgroups of G are those composed of all the operators of G whose orders divide p^β, $\beta < \alpha_1$. The complementary subgroup of such a characteristic subgroup is composed of the p^β power of every operator of G. A necessary and sufficient condition that there are no other characteristic subgroups in G is that all the invariants of G are equal to each other. In this case, the number of the characteristic subgroups, besides the identity, is therefore equal to $\alpha_1 - 1$, and the number of pairs of complementary characteristic subgroups is $(\alpha_1 - 1)/2$ when α_1 is odd. When α_1 is even, the number of these pairs is $(\alpha_1 - 2)/2$ and one of the characteristic subgroups is self-complementary.

It may be desirable to direct attention to the difference between complementary subgroups and subgroups of complementary types. If G is of type $(m_1, m_2, \cdots, m_\lambda)$, and if two of its subgroups are of types $(\alpha_1, \alpha_2, \cdots, \alpha_{\lambda_1})$ and $(\beta_1, \beta_2, \cdots, \beta_{\lambda_2})$ respectively, these subgroups are said to be of complementary types when it is possible to satisfy each of the following equations, where x is either 0 or some α, and y is either 0 or some β and each α or β is used only once*:

$$x + y = m_i \qquad (i = 1, 2, \cdots, \lambda).$$

Subgroups which are of complementary types are clearly also complementary subgroups. That the converse is not necessarily true may be seen by considering the group of type (4, 1). This group contains operators of order p^3 which are not powers of operators of order p^4 and such an operator of order p^3 generates a subgroup whose complementary subgroups are cyclic and of order of p^2 but are not contained separately in cyclic groups of order p^4. Hence $\alpha_1 = \alpha_{\lambda_1} = 3$ and $\beta_1 = \beta_{\lambda_2} = 2$ in the present case, so that neither of the two equations $x + y = m_i$, $(i = 1, 2)$, can be satisfied. The complementary subgroup of the cyclic subgroup of order p^3 which is contained in the cyclic subgroups of order p^4 is of type (1, 1), and in this case the complementary subgroups are also of complementary types.

---

* G. A. Miller, *Transactions of the American Mathematical Society*, vol. 21 (1920), p. 313.

§ 2. *Characteristic subgroups generated by operators of a given order.*

The number of the characteristic subgroups contained in G depends on the number of the different invariants of G but is not affected by the number of these invariants which are equal to each other. That is, if no two of the invariants of G are equal to each other G has exactly the same number of characteristic subgroups as the group G which includes G and has no invariant except such as are equal to those of G, but which has at least two equal invariants. Hence in the study of the number of the characteristic subgroups of G it may be assumed, without loss of generality, that G is of type $(\alpha_1, \alpha_2, \cdots, \alpha_\lambda)$, $\alpha_1 > \alpha_2 > \cdots > \alpha_\lambda$. To emphasize the fact that some invariants may be equal to each other the group G will be replaced by the group G'. Let $\alpha_1 - \alpha_2 = \alpha'_1$.

The cyclic subgroup of order p^r, $r < \alpha'_1$, which is generated by each operator of order p^{α_1} contained in G is evidently a characteristic subgroup of G, and G contains no other cyclic characteristic subgroup whenever $p > 2$. When $p = 2$ and $1 < r < \alpha'_1$, G clearly has two and only two cyclic characteristic subgroups of order p^r. Hence the following theorem: *An abelian group of order p^m cannot have more than one characteristic subgroup of order p. A necessary and sufficient condition that such a group G contains at least one characteristic cyclic subgroup of order p^r, p^r being less than $p^{\alpha'_1}$, is that G' has only one largest invariant. A necessary and sufficient condition that G' contains two cyclic characteristic subgroups of order p^r, $1 < r < \alpha'_1$, is that $p = 2$ and that G' has only one largest and also only one next to the largest invariant. No abelian group of order p^m has more than two characteristic cylic subgroups of the same order.*

From the preceding theorem it results that there is a marked difference as regards characteristic subgroups between the groups whose orders are powers of 2 and those whose orders are powers of an odd prime number. Hence we shall assume in what follows, unless the contrary is stated, that $p > 2$. It is easy to prove that every characteristic subgroup of G which involves operators of order p^r must involve the subgroup generated by all the operators of order p^r which are contained in the cyclic subgroups of order p^{α_1} found in G. Hence this characteristic subgroup will be called *the fundamental characteristic subgroup generated by operators of order p^r.* The fundamental characteristic subgroup noted in the first paragraph of the Introduction may therefore also be called, in accord with this more general nomenclature, the fundamental characteristic subgroup generated by operators of order p.

A characteristic subgroup of G cannot involve any operator of order p^{α_1} since all the operators of highest order contained in G are I-conjugate and every abelian group is generated by its operators of highest order. Every characteristic subgroup of G which involves operators of order p^{α_1-1} must involve the ϕ-subgroup of G since this is composed of all the operators of G which have the property that each of them is the pth power of some other operator of G. Hence the ϕ-subgroup of G is its fundamental characteristic subgroup involving operators of order p^{α_1-1}. When $\lambda > 1$, G has more than one characteristic subgroup which are generated by operators of order p^{α_1-1} These can be arranged linearly so that each contains all those which precede it and involves one more set of I-conjugate operators of order p^{α_1-1} than the one which immediately precedes it.

In fact, the first of these characteristic subgroups is the ϕ-subgroup of G and the remaining $\lambda - 1$ may be obtained by adjoining successively all the operators of smallest order contained in G which are not found in the preceding characteristic subgroup. The complementary subgroups of these characteristic subgroups taken in the reverse order are the λ characteristic subgroups of G which are generated by its operators of order p, and the sum of the numbers of the sets of I-conjugate operators of highest order in each pair formed by one of these characteristic subgroups and its complementary subgroup is $\lambda + 1$. These complementary subgroups are evidently also of complementary types.

All the subgroups of index p under G have the ϕ-subgroup of G for their cross-cut. Hence each such subgroup corresponds to a subgroup of index p in the ϕ-quotient group of G. These subgroups may be divided into λ sets of I-conjugate subgroups corresponding to the λ characteristic subgroups of G which involve only operators of order p. Hence the following theorem: *In any group of order* p^m, *p being a prime number, all the subgroups of index p which are of the same type are I-conjugate.* It may be noted that it is possible to construct prime power abelian groups in which there are subgroups of every other index which are not I-conjugate. In fact, the abelian group of order p^m and of type $(m - 1, 1)$, $m > 2$, contains cyclic subgroups of every index $> p$ which are not I-conjugate.

A direct proof of the italicized theorem of the preceding paragraph is as follows: The independent generators of G' can be so selected that they differ from the possible independent generators of any given subgroup of index p only as regards one operator, and that the pth of this operator is the remaining independent generator of the subgroup in question. If such a selection of the independent generators of two subgroups of index p and of the same type is made a (1, 1) isomorphism between these subgroups may be established so as to make an independent generator of one of these subgroups correspond to an arbitrary independent generator of the same order in the other. Hence these subgroups correspond in some automorphism of G.*

---

* Miller, Blichfeldt, Dickson, *Finite Groups*, 1916, p. 73.

It was noted above that the λ characteristic subgroups of G which are generated by operators of order p^{α_1-1} can be arranged linearly so that each includes all those which precede it and that no two of these characteristic subgroups are of the same type. It will be seen that *no abelian group of order p^m, p being an odd prime number, contains two characteristic subgroups which are of the same type,* but it is not always possible to arrange linearly the characteristic subgroups which are generated by operators of order p^r so that each of these subgroups includes all those which precede it.

To obtain all the characteristic subgroups of G which are generated by operators of order p^r we may begin with the fundamental characteristic subgroup K_r of G which is generated by operators of order p^r. In this characteristic subgroup all the operators of order p^r constitute a single set of I-conjugates. When $\lambda > 1$, a characteristic subgroup whose largest operators are of order p^r and which involves two sets of I-conjugate operators of this order can be obtained by adjoining to K_r the smallest set of I-conjugate operators of lowest order found in G but not in K_r. When this lowest order is p there may be more than one set of I-conjugate operators of lowest order found in G which are not contained in K_r. In this case such sets are added successively in order of magnitude beginning with the smallest. We thus obtain a series of characteristic subgroups which can be arranged linearly so that each includes all those which precede it.

A new series of characteristic subgroup may be started by adjoining to K_r the smallest set of I-conjugate operators of lowest order found in G but not contained in the last subgroup of the preceding series. The first subgroup of this new series K_r' involves two or three sets of I-conjugate operators of order p^r according as it does not or does contain more operators of lowest order than K_r. To obtain the various characteristic subgroups of the second series we adjoin to K_r' the smallest set of I-conjugate operators of lowest order found in G but not in K_r. As all the characteristic subgroups of G can be found by continuing this process it has been proved that no two characteristic subgroups of G are of the same type.

It results from this method for finding all the characteristic subgroups of G that while the number of the characteristic subgroups of G cannot exceed the number of the different types of subgroups found in G it may be less than this number. A necessary and sufficient condition that G contains a characteristic subgroup of type $(r_1, r_2, \cdots, r_\lambda)$, where $r_1 \geqq r_2 \geqq \cdots \geqq r_\lambda$ and one or more of the r's may be 0 is that $r_\gamma - r_{\gamma+1} < \alpha_\gamma - \alpha_{\gamma+1}$ $(\gamma = 1, 2, \cdots, \lambda - 1)$ whenever r_γ and $r_{\gamma+1}$ are different from 0. Hence the following theorems: *The number of the characteristic subgroups of any abelian group G' of order p^m, p being an odd prime number, is equal to the number of the characteristic subgroups in a subgroup G of G' which has for* *its independent generators all the different independent generators of G' but has no two independent generators of the same order. If G is of type $(\alpha_1, \alpha_2, \cdots, \alpha_\lambda)$ then G contains one and only one characteristic subgroup of type $(r_1, r_2, \cdots, r_\lambda)$, $r_1 \geqq r_2 \geqq \cdots \geqq r_\lambda$, where $r_1 < \alpha_1$ and some of the r's may be 0, and $r_\gamma - r_{\gamma+1} \leqq \alpha_\gamma - \alpha_{\gamma+1}$ $(\gamma = 1, 2, \cdots, \lambda - 1)$ whenever r_γ and $r_{\gamma+1}$ are both different from 0.*

To illustrate this theorem it may be noted that the abelian group of order p^{10} and of type 3, 3, 2, 1, 1 contains one and only one characteristic subgroup of each of the following types: (1, 1), (1, 1, 1), (1, 1, 1, 1, 1), (2, 2, 1), (2, 2, 1, 1, 1), (2, 2, 2, 1, 1). Hence this group contains six characteristic subgroups besides the identity, and this is also the number of the characteristic subgroups of the abelian group of order p^6 and of type 3, 2, 1 whenever $p > 2$. These characteristic subgroups are of the following types: (1), (1, 1), (1, 1, 1), (2, 1), (2, 1, 1), (2, 2, 1).

It should be noted that every characteristic subgroup of G' has a complementary characteristic subgroup and this is also of the complementary type. When the characteristic subgroups of G' whose largest operator is of order p^r can be arranged linearly so that each includes all those which precede it their complementary characteristic subgroups can be arranged linearly so that each is included in all those which follow it. In particular, the largest characteristic subgroup whose largest operators are of order p^r has for its complementary subgroup the smallest characteristic subgroup whose largest operators are of order $p^{\alpha_1 - r}$, and vice versa.

In view of the reciprocal relations between the characteristic subgroups of G' it may be assumed without loss of generality that $2r \leqq \alpha_1$. From what precedes there results the following theorem: *The number of the different sets of I-conjugate operators of highest order in any characteristic subgroup whose largest operators are of order p^r, increased by the number of the different sets of I-conjugate operators of highest order in its complementary characteristic subgroup, is equal to one more than the number the characteristic subgroups whose largest operator is of order p^r.* In particular, the sum of the numbers of the different sets of I-conjugate operators of highest order in any characteristic subgroup and its complementary characteristic subgroup is independent of the choice of the former characteristic subgroup when the order of the operators of highest order is fixed.

Number of characteristic subgroups when G is of type $(1, 2, 3, \cdots, m)$.

In order to exhibit clearly a method for determining all the characteristic subgroups of any abelian group it seems desirable to consider separately the special case when G is of type $(1, 2, 3, \cdots, m)$ since the formula representing the total number of these subgroups is comparatively simple in this case. It will be convenient to assume that m may represent an indefinitely large number and to consider separately all the characteristic subgroups, whose operators of highest order is p^r. When r is 1 it is evident that there are m such subgroups and that the orders of these r subgroups are p, p^2, $\cdots$, p^m. The number of sets of I-conjugate operators contained in each of these subgroups is 1, 2, $\cdots$, m respectively. That is, this number is equal to the index of p representing the order of the characteristic subgroup.

When $n = 2$ the smallest characteristic subgroup is of order p^3, since this is the order of the fundamental characteristic subgroup K_2 generated by operators of order p^2. All the operators of order p^2 contained in K_2 are I-conjugate since they are separately powers of operators of order p^m contained in G. This characteristic subgroup involves two of the characteristic subgroups whose operators of highest order are of order p, and if we adjoint to K_2 successively the latter characteristic subgroups which are of orders p^3, p^4, $\cdots$, p^m respectively there result $m - 1$ characteristic subgroups whose operators of highest order are of order p^2. Each of these $m - 1$ characteristic subgroups has only one independent generator of highest order, and each of these subgroups involves one more complete set of I-conjugate operators of order p^2 than the one which precedes it.

The smallest characteristic subgroup of G which has two independent generators of highest order and involves no operator whose order exceeds p^2 is of order p^5, and involves three of the characteristic subgroups of G' which are separately generated by operators of order p. It involves three sets of I-conjugate operators of order p^2. This characteristic subgroup can be extended by means of characteristic subgroups generated by operators of order p just as K_2 was extended except that the first of these extending subgroups is of order p^4. Each such extension increases by two the number of I-conjugate operators of order p^2, and hence the number of the sets of I-conjugate operators of order p^2 found in the last one of these characteristic subgroups is equal to the total number of the characteristic subgroups continued in G and having no more than two independent of highest order, viz., p^2. This number is $m - 1 + m - 2$.

As this process may be continued until all the characteristic subgroups generated by operators of order p^2 have been found it results that the number of such characteristic subgroups which involve exactly α independent generators of order p^2 is $m - \alpha$, $\alpha = 1, 2, \cdots, m - 1$. The total number of these characteristic subgroups is therefore

$$m(m - 1)/2.$$

The total numbers of the characteristic subgroups generated by the operators of orders p and p^2 contained in G are therefore the sums of the terms, of the following series of figurate numbers of orders 0 and 1 respectively:

$$1, 1, 1, \cdots \text{ to } m \text{ terms,}$$

$$1, 2, 3, \cdots \text{ to } m - 1 \text{ terms.}$$

The fundamental characteristic subgroup K_3 of G generated by operators of order p^3 is of order p^6, and involves three characteristic subgroups generated by operators of order p as well as three such subgroups generated by operators of order p^2. The number of the characteristic subgroups which involve K_3 but have only two independent generators of order p^2 is evidently $m - 2$ and these subgroups involve $1, 2, \cdots, m - 2$ sets of I-conjugate operators of order p^3 respectively. The number of the characteristic subgroups of G which involve only one independent generator of order p^3 but three and only three independent generators of order p^2 is $m - 3$, etc. Hence the number of the characteristic subgroups of G which involve K_3 but have separately only one independent generator of order p^3 is the sum of the series $1, 2, \cdots, m - 2$. Similarly it results that the number of the characteristic subgroups of G which involve K_3 and have separately two and only two independent generators of order p^3 is the sum of the series $1, 2, \cdots, m - 3$.

As this process may be continued until the largest characteristic subgroup of G which is generated by operators of order p^3 has been reached, it results that the number of the characteristic subgroups of G which can be generated by operators of order p^3 is the sum of the figurate numbers of the second order, terminating with $m - 2$. The three special cases considered thus far suggest the following theorem: *The number of the characteristic subgroups of G which are separately generated by operators of order p^r is the sum of the figurate numbers of order $r - 1$, terminating with $m - r + 1$.*

This theorem can easily be proved by mathematical induction since the fundamental characteristic subgroup K_r of G generated by operators of order p^r involves r of the characteristic subgroups generated by operators of order p. Those characteristic subgroups of G which involve only one independent generator of order p^r can be found in the same manner as the characteristic subgroups generated by operators of order p^{r-1} were found with the exception that the series of numbers in the present case consists of $m - r + 1$ numbers while in the preceding case it consisted of $m - r + 2$. The sum of the first $m - r + 1$ figurate numbers of order $r - 2$ which constitute the preceding series is therefore the last term of this series.

Similarly, the sum of the first $m - r$ figurate numbers of order $r - 2$ is the next to the last term in the present series, etc. Hence it results that the present series is composed of figurate numbers if the preceding series was composed of such numbers, and hence the proof of the theorem in question, is complete. The fact that the number of the characteristic subgroups generated by operators of order p^r is equal to the number of such subgroups generated by operators of order p^{m-r} follows directly from the properties of figurate numbers* as well as from the (1, 1) correspondence between the characteristic subgroups of complementary types.

In the special case under consideration it is easy to see that the number of the characteristic subgroups generated by operators of order p^r is equal to the number of the sets of I-conjugate operators of this order. Hence the latter number is also the sum of the figurate numbers of order $r - 1$ when G is of type $(1, 2, 3, \cdots, m)$. As was noted above this result is not affected when G has more than one invariant which is equal to p^α, $1 \leqq \alpha \leqq m$.

---

* Cf., P. Bachmann, *Niedere Zahlentheorie,* 1910, p. 10.

ERRATA.

Page 152, in the determinants D_1, D_2, and D_3, in place of $h - 1$, $i - 1$, $2i - h - 1$, etc., read a_{h-1}, a_{i-1}, a_{2i-h-1}, etc.

Page 153, the words "the following figures" immediately above the figures refer to the three lower figures. The two upper figures should be three lines higher up, at the beginning of the paragraph; and the inscriptions "Vanishing parallelogram for n odd," and "Vanishing parallelogram for n even," belong to these two upper figures respectively.